線形符号のゼータ関数とリーマン予想の類似 : Iwan Duursmaの仕事の紹介 (符号と暗号の代数的数理)

AUTHOR(S):

知念, 宏司; 平松, 豊一

CITATION:

知念, 宏司 ...[et al]. 線形符号のゼータ関数とリーマン予想の類似 : Iwan Duursmaの仕事の紹介 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 91-101

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25262

数理解析研究所講究録 1361 巻 2004 年 91-101

線形符号のゼータ関数とリーマン予想の類似

(Iwan Duursma の仕事の紹介)

大阪工業大学 工学部　知念 宏司
Koji Chinen
Department of Mathematics, Faculty of Engineering,
Osaka Institute of Technology.

法政大学 工学部　平松 豊一
Toyokazu Hiramatsu
Department of Systems and Control Engineering,
Faculty of Engineering, Hosei University.

概 要

I. Duursma defined the zeta function for the geometric Goppa code in [1] and later he extended the definition to any linear codes. For self-dual codes, the zeta functions contain deep structures similar to those of algebraic curves and we can formulate an analogue of the Riemann hypothesis. This report is a survey of Duursma's work.

1 導 入

1999 年, 論文 [1] において Iwan Duusma は初めて符号の zeta 関数を定義した. 彼は幾何学的 Goppa 符号の Hamming 重さ分布を考察する過程でそのような着想を得たのであった. その後, 一般の線型符号にまで zeta 関数の定義が拡張され ([2]), 同時にまた, 代数幾何学を用いずに符号理論の言葉のみでその定義や性質を記述する努力が行われた. さらに [3] においては, 自己双対的な線型符号に対して Riemann 予想の類似が定式化されており, 符号の zeta 関数は代数曲線の zeta 関数ときわめてよく似た性質を持つこと, また符号の, 特に重さ分布に関して, 豊かな情報を含むらしいことがわかった. 「らしい」と述べたのは, このテーマがまだ始まったばかりの新しいテーマであり, 非常に多くの未解決問題の宝庫と考えられるためである. また, 代数幾何学とは一応独立に議論できる符号の zeta 関数が, 代数曲線の zeta 関数と同様な性質を持つということもきわめて興味深く, これは線型符号の理論が代数曲線の理論と同程度の深い数学的構造を持つことを示唆しているとも考えられるのである.

本稿は, 文献 [2], [3] を中心に, 符号の zeta 関数に関する Duursma の理論を概観する総合報告である.

2 重さ多項式と zeta 関数

符号の zeta 関数は, 符号の重さ多項式 (weight enumerator) から具体的に構成される. ここで, 重さとは通常の Hamming 重さのことである. p を素数, $q = p^r$ $(r \geq 1)$ とし, C

を有限体 $\mathbf{F}_q$ 上の $[n,k,d]$ 符号とする. また $c \in C$ の Hamming 重さを $\mathrm{wt}(c)$ で表す. よく知られているように,

$$A_i := \sharp\{c \in C\ ;\ \mathrm{wt}(c) = i\}$$

とおくとき,

$$W_C(x,y) := \sum_{i=0}^{n} A_i x^{n-i} y^i$$

を C の重さ多項式と呼ぶ. これは x, y の斉次 n 次式である. このとき, 符号の zeta 関数は次のように定義される:

定 義 2.1 C に対して, 次数 $n-d$ 以下のある多項式 $P(T) \in \mathbf{Q}[T]$ がただ 1 つ存在して,

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{W_C(x,y)-x^n}{q-1}T^{n-d} + \cdots$$

が成立する. $P(T)$ を C の **zeta 多項式**, $Z(T) := P(T)/\{(1-T)(1-qT)\}$ を C の **zeta 関数**と呼ぶ.

この定義はやや解りづらいので, 多少説明が必要であろう. まずこの等式をどう見るかだが, 左辺は T の有理式なので, これは原点のまわりでのべき級数展開を利用する. つまり

$$\begin{aligned} \frac{1}{1-T} &= 1+T+T^2+\cdots, \\ \frac{1}{1-qT} &= 1+qT+q^2T^2+\cdots \end{aligned}$$

とし, 左辺を

$$P(T)(1+T+T^2+\cdots)(1+qT+q^2T^2+\cdots)(y(1-T)+xT)^n$$

の形に変形する. これは明らかに原点の近傍で正則だから (例えば $|T| < 1/q$ の範囲で考えればよい), 「展開して項を並べ換える」計算が許される. こうして T に関して昇べきの順に並べ換えたものが右辺のような形になる, すなわち T^{n-d} の係数に C の重さ多項式が現れるようになる, というのが上の等式の意味である.

これで定義の等式の言わんとすることはわかるのだが, そのような $P(T)$ が本当に一意的に存在するのだろうか, という点については, やはり証明が必要であろう. それを以下に述べよう. まず,

$$f(T) := \frac{(y(1-T)+xT)^n}{(1-T)(1-qT)}$$

という関数を考える. つまり, 定義 2.1 で $P(T)=1$ とした場合である. これの $T=0$ のまわりのべき級数展開を

$$\left\{\sum_{j=0}^{n}\binom{n}{j}(x-y)^j y^{n-j}T^j\right\}(1+c_1T+c_2T^2+\cdots)$$

とおく. つまり { } の中は $(y(1-T)+xT)^n=((x-y)T+y)^n$ の (T の多項式としての) 2 項展開, $(1+c_1T+c_2T^2+\cdots)$ は $1/\{(1-T)(1-qT)\}$ のべき級数展開を整理したものである. これをさらに展開して $1, T, T^2, \cdots, T^{n-d}$ の係数を調べる. すると, 適当な整数 b_{ij} が存在して,

$$\begin{array}{ll} 1 \text{ の係数 (定数項)} & y^n \\ T \text{ の係数} & nxy^{n-1}+(c_1-n)y^n \\ \cdots\cdots & \cdots\cdots\cdots \\ T^i \text{ の係数} & b_{i0}x^iy^{n-i}+b_{i1}x^{i-1}y^{n-i+1}+\cdots+b_{ii}y^n \\ \cdots\cdots & \cdots\cdots\cdots \\ T^{n-d} \text{ の係数} & b_{n-d,0}x^{n-d}y^d+b_{n-d,1}x^{n-d-1}y^{d+1}+\cdots+b_{n-d,n-d}y^n \end{array} \tag{2.1}$$

となることが簡単な計算からわかる. そこで今度は, 有理数 $a_0, a_1, \cdots, a_{n-d}$ が与えられているとして, $(a_0+a_1T+\cdots+a_{n-d}T^{n-d})f(T)$ の T^{n-d} の係数を見てみよう. それは

$$\begin{array}{r} a_{n-d}y^n \\ +a_{n-d-1}\{xy^{n-1}+(c_1-n)y^n\} \\ \cdots\cdots\cdots \\ +a_0\{b_{n-d}x^{n-d}y^d+\cdots+b_1xy^{n-1}+b_0y^n\} \end{array}$$

であることがわかる. 一方, $(W_C(x,y)-x^n)/(q-1)=(A_dx^{n-d}y^d+\cdots+A_ny^n)/(q-1)$ であるから, これらを比較すると, 上の $a_0, a_1, \cdots, a_{n-d}$ を順次決めていくことができる (しかも可能性は 1 通り). 正確に言えば, (2.1) において $b_{00}=1$ (定数項 y^n の係数 1 をこうおく), $b_{10}=n$, $b_{11}=c_1-n$ とすると, 上の $a_0, \cdots, a_{n-d}$ は連立 1 次方程式

$$\begin{bmatrix} b_{n-d,0} & 0 & \cdots & \cdots & 0 \\ b_{n-d,1} & b_{n-d-1,0} & 0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ & & & \ddots & 0 \\ b_{n-d,n-d} & b_{n-d-1,n-d-1} & \cdots & & b_{00} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-d} \end{bmatrix} = \frac{1}{q-1} \begin{bmatrix} A_d \\ A_{d+1} \\ \vdots \\ \vdots \\ A_n \end{bmatrix}$$

の解となるが, 各対角成分 b_{i0} は 2 項係数 $\binom{n}{i}$ に等しいことがわかり, したがって解はつねに一意的に存在するのである. そこで $a_0+a_1T+\cdots+a_{n-d}T^{n-d}=P(T)$ とすればよいことがわかる.

この証明から, zeta 多項式 $P(T)$ の存在に関しては, $W_C(x,y)$ が実在する符号の重さ多項式であることよりも, それが x, y の斉次 n 次式であることがより本質的であることがわかる. これに関連して, **MDS 符号** (最大距離分離符号) とその重さ分布について指摘しておくことはあとの議論にとっても有用であろう.

$[n,k,d]$ 符号 C に対して $d=n-k+1$ が成り立つとき, C を MDS 符号であるという. これは Singleton の限界式 $d\le n-k+1$ で等号が成立する場合である. 条件 $d=n-k+1$ の影響で, MDS 符号の重さ分布は n, d のみで決まってしまう ([5, Ch. 11 §3]). そこで,

MDS 符号の重さ多項式を $M_{n,d}(x,y)$ と表す. 形式的に計算すると, $M_{n,d}(x,y)$ は負の係数を持つこともある. もちろん, そのようなときには対応する符号は実在しないこととなる. しかしその場合も, $M_{n,d}(x,y)$ は x, y の斉次 n 次式であるから, その zeta 多項式を定義することができる. 実は, 次が成り立つ:

命 題 2.2 MDS 符号の zeta 多項式は $P(T)=1$ である. 逆に, $P(T)=1$ を zeta 多項式にもつ符号は MDS 符号である.

証 明. [2, p.59]. ∎

この命題から容易に次が得られる:

系 2.3 任意の $[n,k,d]$ 符号 C とその重さ多項式 $W_C(x,y)$ に対して, その zeta 多項式を $P(T)=a_0+a_1T+\cdots+a_rT^r$ とすると,

$$W_C(x,y)=a_0M_{n,d}(x,y)+a_1M_{n,d+1}(x,y)+\cdots+a_rM_{n,d+r}(x,y).$$

上の系は, zeta 多項式を重さ多項式によって書き換えたものと見ることができる. Zeta 多項式の考察によって初めて, MDS 符号の重さ多項式と, 実在の符号の重さ多項式とのこのような関係が明らかにされたと言ってよいだろう.

最後に, 代数曲線の zeta 関数について簡単にまとめておこう. $\mathcal{C}$ を $\mathbf{F}_q$ 上のなめらかな代数曲線とし,

$$N_m := \sharp\{\mathcal{C} \text{ 上の } \mathbf{F}_q \text{ 有理点}\}$$

とすると, $\mathcal{C}$ の zeta 関数は

$$\mathcal{Z}(t)=\exp\Big(\sum_{m=1}^{\infty}N_m\frac{t^m}{m}\Big)$$

で定義される. そして実は

$$\mathcal{Z}(t)=\frac{\mathcal{P}(t)}{(1-t)(1-qt)}$$

となる多項式 $\mathcal{P}(t)\in\mathbf{Z}[t]$ が存在することが示される (この $\mathcal{P}(t)$ を $\mathcal{C}$ の zeta 多項式とよぶ).

3 いくつかの性質

C は $\mathbf{F}_q$ 上の $[n,k,d]$ 符号であるとする. C の双対符号 $C^\perp$ は

$$C^\perp := \{u\in{\mathbf{F}_q}^n\ ;\ u\cdot v=0, \forall v\in C\}$$

で定義される. ただし, $u=(u_1,u_2,\cdots,u_n), v=(v_1,v_2,\cdots,v_n)\in{\mathbf{F}_q}^n$ に対して, $u\cdot v=u_1v_1+u_2v_2+\cdots+u_nv_n$ である. $C^\perp$ の次元, 最小距離をそれぞれ $k^\perp(=n-k)$, $d^\perp$ と表す. また, C が自己双対符号であるとは $C^\perp=C$ であるときにいう.

まず, (自己双対とは限らない) 一般の線型符号の zeta 関数に関する性質をまとめる:

定 理 3.1 C の zeta 多項式を $P(T)$ とする.

(1) $\deg P(T) = n + 2 - d - d^{\perp}$

(2) $C^{\perp}$ の zeta 多項式, zeta 関数をそれぞれ $P^{\perp}(T)$, $Z^{\perp}(T)$ とすると,

$$\begin{aligned} P^{\perp}(T) &= P\Big(\frac{1}{qT}\Big)q^{g}T^{g+g^{\perp}}, \\ Z^{\perp}(T) &= Z\Big(\frac{1}{qT}\Big)q^{g-1}T^{g+g^{\perp}-2} \end{aligned}$$

が成り立つ. ただし,

$$\begin{aligned} g &:= n+1-k-d, \\ g^{\perp} &:= n+1-k^{\perp}-d^{\perp}(=k+1-d^{\perp}). \end{aligned}$$

特に, C が自己双対なら, $P(T) = P^{\perp}(T)$ により,

(1)′ $\deg P(T) = 2g$.

(2)′ **関数等式**

$$\begin{aligned} P(T) &= P\Big(\frac{1}{qT}\Big)q^{g}T^{2g}, \\ Z(T) &= Z\Big(\frac{1}{qT}\Big)q^{g-1}T^{2g-2} \end{aligned}$$

が成り立つ.

Duursma は代数曲線の場合の類似から g を C の種数 (genus) と呼んでいる. ただし, その数学的 (符号理論的) 意味付けはまだ不明ということである. また, 関数等式が成り立つのが一般には C が自己双対のときに限られることも注目に値する.

証明には MacWilliams の恒等式

$$W_{C^{\perp}}(x,y) = \frac{1}{\sharp C}W_{C}(x+(q-1)y, x-y)$$

([5, p.146, Th. 13]) および MDS 重さ多項式の性質 (系 2.3) が用いられる (*cf.* [2, p.59]).

代数曲線の zeta 多項式 $\mathcal{P}(t)$, zeta 関数 $\mathcal{Z}(t)$ の場合の, 対応する結果は次の通りである. $\mathcal{C}$ の種数を g とすると, まず $\deg \mathcal{P}(t) = 2g$ であり, 関数等式は

$$\begin{aligned} \mathcal{P}(t) &= \mathcal{P}\Big(\frac{1}{qt}\Big)q^{g}t^{2g}, \\ \mathcal{Z}(t) &= \mathcal{Z}\Big(\frac{1}{qt}\Big)q^{g-1}t^{2g-2} \end{aligned}$$

となる.

4 自己双対符号に対する Riemann 予想の類似

代数曲線の zeta 関数 については, 「Riemann 予想」と呼ばれる命題 (Weil によって証明された) が知られている. それは

$$\mathcal{P}(t) \text{ の任意の根 } \alpha \text{ に対して, } |\alpha| = \frac{1}{\sqrt{q}}$$

というものである. 前節の結果から, 自己双対符号の zeta 関数 $P(T)$ に対しても, 同様の命題を述べることができる. それを述べる前に 1 つの定理を見ておこう:

定 理 4.1 C を (自己双対とは限らない) $\mathbf{F}_q$ 上の $[n,k,d]$ 線型符号, $P(T)$ をその zeta 多項式とする. $P(T) = a_0(1 + aT + \cdots)$ の形に書いたとき,

$$d + 1 \leq q + 1 + a$$

が成り立つ.

証 明. [3, p.118]. ∎

$P(T)$ の根を $\alpha_1, \alpha_2, \cdots, \alpha_r$ とすると,

$$a = -\sum_{j=1}^{r} \frac{1}{\alpha_j}$$

であるから, $P(T)$ **の根の大きさの評価は** C **の最小距離の評価を与える**ことがわかる.

さて, C が自己双対のときは, $P(T)$ は $2g$ 個の根を持つ (定理 3.1 (1)′). さらに, 必要なら番号をつけかえて, それらの根を

$$\alpha_1\alpha_2 = \alpha_3\alpha_4 = \cdots = \alpha_{2g-1}\alpha_{2g} = \frac{1}{q}$$

が成り立つようにできる (この議論は初等的にでき, 代数曲線の場合と全く同じである. 例えば [7, p.167]). そこで, 自己双対符号に対する Riemann 予想は, 代数曲線との類似を考えれば, 次のように定式化するのが適当であろう:

定 義 4.2 C を自己双対符号, その zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, C は Riemann 予想を満たすという.

Duursma は, 代数曲線の場合の単純な類似だけではなく, 数多くの数値実験の結果から, よい符号が概してこの Riemann 予想を満たしていることを実際に観察し, このような定式化に至ったようである.

C が Riemann 予想を満たす自己双対符号であれば,

$$d+1 \leq q+1+2g\sqrt{q} \tag{4.1}$$

という, 最小距離の評価が得られることになる. これは代数曲線の場合の Hasse-Weil 限界式に対応するものである. つまり, 代数曲線 $\mathcal{C}$ の zeta 多項式を $\mathcal{P}(t) = 1 + at + \cdots$ の形に書くとき, $\mathcal{C}$ の $\mathbf{F}_q$ 有理点の個数 N は

$$N = q+1+a$$

と表され, $\mathcal{C}$ に対する Riemann 予想からは

$$N \leq q+1+2g\sqrt{q} \quad (g:\ \mathcal{C} \text{ の種数}) \tag{4.2}$$

が得られ, この不等式を Hasse-Weil 限界式と呼ぶのである. (4.2) 式は整数論, 代数幾何学において (もちろん符号理論においても) 大変よく使われる重要な評価式である. 一方, (4.1) 式は, 実はこれだけでは最小距離の満足な評価を与えるものではないのである. そこで, 有用な評価を得るには, Riemann 予想以外の仮定が必要になるのだが, それについては最後の節で述べることにして, ここでは Riemann 予想自体についてさらに詳しく考えよう.

実は, 符号の zeta 関数についての最も大きな未解決問題は,

問 題 4.3 Riemann 予想を満たす自己双対符号とはどのようなものか定式化せよ.

というものである. Duursma 自身も膨大な数値実験によりいくつかの観察を行なっているようだが, まだ自己双対符号が Riemann 予想を満たすための条件を得るには至っていないようである. 最も興味深い観察を問題の形で述べよう:

問 題 4.4 「Extremal な自己双対符号は Riemann 予想を満たす」は正しいか.

Duursma は論文 [3] で, このことを "prove or disprove" (証明するか反証をあげよ) と書いており, 「予想」というほどの肯定的な数学的根拠がまだ十分揃っていないことを窺わせる.

この問題についても若干の説明が必要であろう. 自己双対符号 C が extremal であるとは, C が可能な最大の最小距離を実際に持っていることをいう. 正確に言えば, まず符号長 n の自己双対符号の最小距離の評価として, 次の Mallows-Sloane 限界式が知られている:

$$d \leq 2\left[\frac{n}{8}\right] + 2, \tag{4.3}$$

$$d \leq 4\left[\frac{n}{24}\right] + 4, \tag{4.4}$$

ただし, (4.3) 式は自己双対 2 元符号一般に対する評価, (4.4) 式は重偶な ($\Leftrightarrow$ すべての符号語に対し, その Hamming 重さが 4 で割れる) 自己双対 2 元符号に対する評価である. Extremal な自己双対符号とは, この Mallows-Sloane 限界式で等号が成り立つもののことである ([6, p.139]). なお, 重偶な自己双対 2 元符号を **II 型**の符号 (type II code) と呼ぶことが多い.

上記の観察の根拠となったいくつかの具体例を, zeta 多項式の実際的計算法とともに, 節をあらためて見ていこう.

5 いくつかの具体例

C を $\mathbf{F}_q$ 上の $[n,k,d]$ 符号とする. C の zeta 多項式 $P(T)$ を実際に計算するには, 次の**正規化重さ多項式** (normalized weight enumerator) を使うのが便利である:

定 義 5.1 ([2], [3])
$W_C(x,y)=\sum_{i=0}^{n}A_ix^{n-i}y^i$ に対し,

$$a(t):=\frac{1}{q-1}\sum_{i=d}^{n}\frac{A_i}{\binom{n}{i}}t^{i-d}$$

を C の正規化重さ多項式という.

これに対して, 次が成り立つ:

定 理 5.2

$$\frac{P(T)}{(1-T)(1-qT)}(1-T)^{d+1}\equiv a\Big(\frac{T}{1-T}\Big)\ (\mathrm{mod}\ T^{n-d+1}). \tag{5.1}$$

証 明. [2, p.63]. ∎

もちろんこの場合も, 原点のまわりのべき級数展開を考え, 級数としての合同式と考えるのである. $a(t)$ は $W_C(x,y)$ から容易に計算できるので, (5.1) の両辺において $1, T, \cdots, T^{n-d}$ の係数を比較して $P(T)$ を決めていけばよい.

例 5.3 $[8,4,4]$ 拡大 Hamming 符号 C_8 ([4, p.112], [6, p.35] 等). これは自己双対な 2 元符号であり, extremal, しかも重偶と, よい特徴をそなえた符号の 1 つである. 重さ多項式は $W_{C_8}(x,y)=x^8+14x^4y^4+y^8$ であり ([6, p.135]), 正規化重さ多項式は

$$a(t)=\frac{1}{5}+t^4$$

と計算される. また種数は $g=n+1-k-d=1$ なので $\deg P(T)=2$, そこで $P(T)=a_0+a_1T+a_2T^2$ とおく. 定理 5.2 によって

$$(a_0+a_1T+a_2T^2)(1+T+T^2+\cdots)(1+2T+4T^2+\cdots)(1-T)^5$$

$$\equiv\frac{1}{5}+T^4(1+T+T^2+\cdots)^4\ (\mathrm{mod}\ T^5)$$

が成り立つから, 係数比較により,

$$P(T)=\frac{1}{5}(1+2T+2T^2)$$

が得られる. $P(T)$ の根は $\alpha=(-1\pm i)/2$ なので, これは $|\alpha|=1/\sqrt{2}=1/\sqrt{q}$, すなわち Riemann 予想を満たす.

その他の興味深い例として次のものを挙げておこう:

(1) 自己双対 $[72,36,16]$ 符号. これは extremal な II 型符号である. 条件から重さ多項式は確定するが, この符号が実在するかどうかはまだ知られていない ([6, p.139]). しかし, 重さ多項式が決まれば zeta 多項式も決まる. Duursma は, この場合も Riemann 予想は成り立つと述べている ([3, p.119], ただし詳細は公表されていない).

(2) 直和符号 $C_8 \oplus C_8 \oplus C_8$. これは 拡大 Hamming 符号を 3 つ「連ねた」符号であり, $[24,12,4]$ というパラメータをもつ (集合としては C_8 3 つの直積集合であるが, このような作り方をするものは通常 "direct sum code" と呼ばれている. *cf.* [5, p.76]). この場合, II 型ではあるが extremal ではない. そして Duursma によれば, Riemann 予想は成り立たないという ([3, p.119]).

(3) 直和符号 $C := C_2 \oplus C_2 \oplus \cdots \oplus C_2$, ただし C_2 は $[2,1,2]$ というパラメータをもつ 2 元符号で, 最も簡単な自己双対符号である. またこれは, 自明な MDS 符号の 1 つでもある. $W_{C_2}(x,y) = x^2 + y^2$ だから, C が m 個の C_2 の直和符号なら $W_C(x,y) = (x^2+y^2)^m$ となる. これらの符号に対しても Riemann 予想が成り立つことが観察されている. しかし C は $n = 4, 6$ 以外 extremal ではなく, また一般に II 型でもない. この符号の特徴は, 上述のように Hamming 重さが 2 項分布する ($\Leftrightarrow$ 重さ多項式が $(x^2+y^2)^m$ $(\exists m \in \mathbf{N})$ の形となる), ということなのである.

これらを含めたいくつかの例を, 符号長の小さいものから順に表にまとめてみた. なお, 表において RH とは Riemann 予想の成立 (○), 不成立 (×) を表し, コメント欄には上に述べたような各性質をもつかどうかを記してある (特に, Hamming 重さが 2 項分布することを "binomial" と表した):

n	符号	パラメータ	重さ多項式	$P(T)$	RH	コメント
2	C_2	$[2,1,2]$	x^2+y^2	1	−	trivial MDS
4	$C_2 \oplus C_2$	$[4,2,2]$	$(x^2+y^2)^2$	$\frac{1}{3}(1+2T^2)$	○	extremal binomial
6	$C_2 \oplus C_2 \oplus C_2$	$[6,3,2]$	$(x^2+y^2)^3$	$\frac{1}{5}(1+4T^4)$	○	extremal binomial
8	C_8 (拡大 Hamming)	$[8,4,4]$	$x^8+14x^4y^4+y^8$	$\frac{1}{5}(1+2T+2T^2)$	○	extremal type II
8	$C_2 \oplus C_2 \oplus C_2 \oplus C_2$	$[8,4,2]$	$(x^2+y^2)^4$	$\frac{1}{35}(5-2T^2-4T^3$ $-4T^4+40T^6)$	○	binomial
10	$C_8 \oplus C_2$	$[10,5,2]$	$(x^8+14x^4y^4+y^8)$ $\cdot(x^2+y^2)$	$\frac{1}{45}(1+2T^2+4T^3+6T^4$ $+8T^5+8T^6+16T^8)$	×	
24	$C_8 \oplus C_8 \oplus C_8$	$[24,12,4]$			×	type II
72	(存在は不明)	$[72,36,16]$			○	extremal type II

6 相対最小距離の漸近的限界式

第 4 節において, 定理 4.1 と Riemann 予想だけでは, 最小距離の評価として満足なものが得られないことを述べた (*cf.* (4.1) 式). ところが, Riemann 予想とともに, より強い条件を仮定すれば, 相対最小距離 d/n のより厳しい漸近的評価が得られる. 本節では, 講演で時間の関係から述べられなかったこの問題について論じよう. まず 1 つの定義を導入する.

定 義 6.1 複素数の集合 $\Omega = \{\omega_1, \omega_2, \cdots, \omega_{2g}\}$ が正 Weil 系 (positive Weil system) をなすとは, 次の (a) ~ (e) が成り立つことである:

(a) すべての $\omega_j \in \Omega$ は代数的整数である.
(b) $\omega_j \in \Omega$ ならば $\overline{\omega_j} \in \Omega$ である.
(c) $\omega_j \in \Omega$ が実数なら, ω_j の Ω での重複度は偶数である.
(d) すべての $\omega_j \in \Omega$ に対して $|\omega_j| = \sqrt{q}$.
(e) $\frac{(1-\omega_1 T)\cdots(1-\omega_{2g}T)}{(1-T)(1-qT)} = \prod_{m=1}^{\infty}(1-T^m)^{-B_m}$ とするとき, すべての $B_m \geq 0$.

定義 6.1 において, (a) ~ (d) が成り立つ場合には, Ω を単に Weil 系と呼ぶ. また, Ω が符号の zeta 多項式 $P(T)$ の根の逆数全体の集合であるなら, (d) が Riemann 予想となる. さて, $m \to \infty$ のとき符号長が無限に大きくなるような自己双対符号 C_m の無限列を考える. このとき,

定 理 6.2 任意の m に対して C_m の zeta 多項式 $P_m(T)$ について, その根の逆数全体の集合が正 Weil 系をなすならば,

$$\limsup_{m\to\infty} \frac{d_m}{n_m} \leq \frac{1}{2} - \frac{1}{2\sqrt{q}},$$

ただし, n_m, d_m はそれぞれ C_m の符号長, 最小距離を表す.

この定理で $q = 2$ の場合を考えると,

$$\limsup_{m\to\infty} \frac{d_m}{n_m} \leq \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 0.146$$

が得られ, これは従来知られている限界式, 例えば II 型符号に対する

$$\limsup_{m\to\infty} \frac{d_m}{n_m} \leq \frac{1}{6} \approx 0.167$$

(Mallows-Sloane 限界, (4.4) から得られる) よりもよくることがわかる.

しかしこの場合も, どのような符号列に対してこれが成り立つのかが問題である:

問 題 6.3 Zeta 多項式 $P(T)$ の根の逆数全体の集合が正 Weil 系をなす符号を特徴づけよ.

これは問題 4.4 と並んで, 最も大きな未解決問題の 1 つである.

なお, 定理 6.2 は, 代数曲線の場合の Drinfeld-Vladut 限界式

$$\limsup_{g\to\infty} \frac{N}{g} \leq \sqrt{q} - 1$$

(N: $\mathbf{F}_q$ 有理点の個数, g: 種数) の類似である.

参考文献

[1] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[2] _____ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[3] _____ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[4] 平松 豊一 : 応用代数学, 裳華房, 1997.

[5] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[6] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).

[7] Stichtenoth, H. : Algebraic Function Fields and Codes, Springer Verlag, 1993.